IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA, v. ANFERNEE CRUZ-FAJARDO, Defendant.	CRIMINAL CASE NO. 1:16-CR-14-TCB-LTW

MAGISTRATE JUDGE'S ORDER AND NON-FINAL REPORT AND RECOMMENDATION

Pending before this Court are Defendant Anfernee Cruz-Fajardo's Motion to Dismiss the Indictment (Doc. 33) and Motion to Suppress evidence (Doc. 34). For the reasons outlined below, Defendant's Motion to Dismiss the Indictment and Motion to Suppress should be **DENIED**. (Docs. 33, 34). Defendant's request for a hearing on the Motion to Dismiss the Indictment is **DENIED**. (Doc. 33).

MOTION TO SUPPRESS

This case concerns whether a magistrate judge in the Eastern District of Virginia may lawfully authorize a warrant for the installation of a Network Investigative Technique ("NIT") on a website allegedly containing pornographic images within her district so that the NIT may deploy malware on computers inside and outside her district for the purpose of ascertaining the identities of individuals frequenting the site.

Defendant maintains that such a warrant exceeded the magistrate's jurisdiction under Rule 41(b) of the Federal Rules of Criminal Procedure and that evidence gained as a result should be suppressed. The Government contends that the warrant was lawful under Rule 41(b)(4) because, in effect, it authorized a tracking device.

I. BACKGROUND

A. The Target Website and the TOR Network

Between September 16, 2014, and February 3, 2015, FBI Special Agents in the District of Maryland investigated what they believed to be a child pornography website ("the Target Website"). (Def.'s Ex. A ¶ 11). The Target Website appeared to be a message board with the primary purpose of advertising and distributing child pornography. (Def.'s Ex. A ¶ 11). The Target Website posted statistics which indicated that it contained a total of 95,148 posts, 9,333 total topics, and 158,094 total members. The main page of the Target Website contained two images depicting partially clothed prepubescent females with their legs spread apart. (Def.'s Ex. A ¶ 12). To the right of the site name on the home page, two data entry fields and a corresponding Login with the message, "Warning! Only registered members are allowed to access the section. Please login below or register an account." (Def.'s Ex. A ¶ 12). The site then contained a hyperlink for registering an account. When the hyperlink was selected, the following message was displayed:

> VERY IMPORTANT. READ ALL OF THIS PLEASE
>
> I will add to this as needed.

> The software we use for this forum requires that new users enter an email address, and checks that what you enter looks approximately valid. We can't turn this off but the forum operators do NOT want you to enter a real address, just something that matches the xxx@yyy.zzz.pattern. No confirmation email will be sent. This board has been intentionally configured so that it WILL NOT SEND EMAIL, EVER. Do not forget your password, you won't be able to recover it.
>
> After you register and login to this forum you will be able to fill out a detailed profile. For your security you should not post information here that can be used to identify you.
>
> . . .
> Note that it is impossible for the staff or owners of this forum to confirm the true identity of users or monitor in realtime all messages posted, and as such we are not responsible for the content posted by those users. You remain solely responsible for the content of your posted messages.

(Def.'s Ex. A ¶ 13). A sampling of the topics available on the Target Website included "Jailbait - Boy," "Jailbait-Girl," "Family -Incest," "Toddlers," etc. (Def.'s Ex. A ¶ 14). FBI investigators believed that the private message function of the site was being used to communicate regarding the dissemination of child pornography. (Def.'s Ex. A ¶ 22). The image and file hosting features allowed users of the Target Website to upload links to images and videos of child pornography that are accessible to all registered users of the Target Website. (Def.'s Ex. A ¶¶ 23-24).

The Target Website was accessible on TOR, which stands for "the onion router," a network that provides anonymity to internet users accessing the site. (Def.'s Ex. A ¶¶ 6-8; Gov't's Br. 2). The TOR software protected the user's privacy by bouncing their communications around a distributed network of relay computers run by volunteers around the world which masked the user's actual IP address, which could otherwise be

used to identify a user. (Def.'s Ex. A ¶ 8). In order to access the TOR network, the user was required to install TOR software either by downloading an add-on to the user's web browser or by downloading the free browser bundle. (Def.'s Ex. A ¶¶ 7-8). The Target Website was a hidden service and did not reside on the traditional or open internet. (Def.'s Ex. A ¶ 10). The Target Website could only be accessed via the TOR network; thus a user could not simply perform a Google search to locate the Target Website. (Def.'s Ex. A ¶ 10).

Even after connecting the TOR network, the user had to know the web address of the website in order to access the Target Website. (Def.'s Ex. A ¶ 10). A user could obtain the web address for the Target Website by communicating with other users on the Target Website's bulletin board, from internet postings describing the sort of content available on the website as well as the website's location, or a hidden services page dedicated to pedophilia and child pornography. (Def.'s Ex. A ¶ 10). Thus, according to the FBI, it is extremely unlikely that any user could simply stumble upon the Target Website without understanding its purpose and content as accessing the website requires numerous affirmative steps by the user. (Def.'s Ex. A ¶ 10).

B. The FBI Obtains a Warrant to Install Malware Affecting Users Logging Into the Target Website

In January 2015, the FBI, acting pursuant to a warrant, seized a copy of the TOR server which hosted the Target Website and ultimately seized control of the Target Website pursuant to a second warrant. (Def.'s Ex. A ¶¶ 28-30). Rather than shutting

the website down, the FBI continued to operate it from a government-controlled computer server in Newington, Virginia, in an attempt to identify and prosecute users throughout the country. (Def.'s Ex. A ¶ 30; Def.'s Ex. C ¶ 11, 24). On February 20, 2015, the FBI obtained a warrant from a magistrate judge in the Eastern District of Virginia in order to deploy the "Network Investigative Technique" or "NIT" software onto the Target Website in the Eastern District of Virginia so that the FBI could investigate any user or administrator who logged into the Target Website by entering a user name and password. (Def.'s Ex. A ¶¶ 30-32). According to the FBI, the NIT operates as follows:

> In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by the warrant, the Target Website, which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the Target Website, . . . the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant . . . and the warrant authorizes obtaining no other information. The NIT will not deny the user of the "activating" computer access to any data or functionality of the user's computer.

(Def.'s Ex. A ¶ 33). Among other information, the NIT will provide the activating computer's IP address, the activating computer's host name, which is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, the activating computer's active operating system username, and the activating computer's Media Access Control ("MAC")

address, which is an address from the computer's network adaptor. (Def.'s Ex. A ¶ 34). The warrant permitted FBI agents to deploy the NIT on the Target Website in the Eastern District of Virginia for up to thirty days. (Def.'s Ex. A ¶ 36). The FBI ended up closing down the Target Website approximately twelve days later. (Def.'s Ex. C ¶ 11).

C. The NIT Leads Law Enforcement to Defendant

According to the FBI, based on data obtained from logs on the Target Website, monitoring by law enforcement, and the deployment of the NIT, the FBI discovered that a user with the name nonamenoname browsed images of prepubescent girls involved in sexual activity on the Target Website on March 2, 2015. (Def.'s Ex. C ¶¶ 27-30). The NIT also determined the user's IP address and that the host name for the user nonamenoname was Heisenberg and the computer login was Anfernee. (Def.'s Ex. C ¶ 27). The FBI asserts that using publicly available websites, FBI Special Agents were able to determine that the user's IP address was operated by the internet service provider Comcast Cable. (Def.'s Ex. C ¶ 32). The FBI then served an administrative subpoena on Comcast Cable and learned from Comcast that Brandon Cannon was assigned to the IP address. (Def.'s Ex. C ¶ 32). On June 30, 2015, law enforcement observed a vehicle registered to Andrew Jackson Cannon parked outside of a Decatur apartment. (Def.'s Ex. C ¶ 33). The FBI believed the vehicle was driven by Brandon Cannon. (Def.'s Ex. C ¶ 33). Based on this information, the FBI obtained a warrant on July 13, 2015, from a magistrate judge in the Northern District of Georgia for the search of the apartment.

(Def.'s Ex. C, at 1). According to the Government, after agents subsequently searched the apartment, Defendant Cruz-Fajardo admitted that he had accessed the Target Website and exculpated his two roommates. (Gov't's Br. 6-7).

On January 12, 2016, a federal grand jury indicted Defendant Anfernee Cruz-Fajardo for knowingly receiving a visual depiction of a minor engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(2) and (b)(1) and for knowingly possessing at least one or more computers and computer storage devices which contained one or more visual depictions of minors engaged in sexually explicit conduct involving at least one prepubescent minor and at least one minor who had not attained twelve years of age in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2).

II. LEGAL ANALYSIS

Defendant contends that the magistrate judge in the Eastern District of Virginia who authorized deployment of the NIT exceeded her jurisdiction to do so under Rule 41 of the Federal Rules of Criminal Procedure.[1] In support, Defendant argues the warrant's reach was extraterritorial because it allowed for the installation of the NIT on

[1] Although Defendant also argues in a perfunctory fashion that the magistrate judge in the Eastern District of Virginia had no authority to issue the warrant under the Federal Magistrates Act, Defendant focuses his argument on the magistrate judge's authority under Rule 41(b)(1) of the Federal Rules of Criminal Procedure. Defendant does not include any analysis as to the magistrate judge's jurisdiction under the Federal Magistrate's Act. Accordingly, this Court has also focused its analysis upon the magistrate judge's jurisdiction pursuant to Rule 41(b)(1). Because Defendant's Motion to Suppress is resolved on the issues of the law enforcement officers' good faith and whether the exclusionary rule should apply under the circumstances, consideration of the magistrate judge's authority under the Federal Magistrate's Act would not change the result.

computers which were physically located outside of the Eastern District of Virginia. Defendant contends that because the magistrate judge exceeded her jurisdiction, the warrant was void ab initio and evidence that was obtained as a result of the warrant should be suppressed. The Government argues in response that the warrant may operate extraterritorially because Rule 41 permits a magistrate judge to issue a warrant to install a tracking device within the district even though the tracking device is used to track the movement of persons or property outside the district. Fed. R. Crim. P. 41(b)(4).

Under Rule 41(b)(1) of the Federal Rules of Criminal Procedure, a magistrate judge has the authority to issue a warrant to search for and seize a person or property located within the magistrate judge's district. Fed. R. Crim. P. 41(b)(4). The Rule allows for magistrates to issue warrants which have reach outside the district only where (1) the person or property initially is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed; (2) the investigation concerns terrorism and activities related to the terrorism have occurred within the magistrate judge's jurisdiction; (3) the warrant is for the installation of a tracking device on property located within the district; or (4) activities related to the crime occurred within the magistrate judge's district, but the property is in a United States territory, possession, or commonwealth, the premises are owned by a United States diplomatic mission in a foreign state, or a residence or land owned or leased by the United States and used by United States personnel assigned to a United States

diplomatic or consular mission in a foreign state.[2] Fed. R. Crim. R. 41(b). The Government argues the warrant may lawfully reach extraterritorially under Rule 41 because the NIT operates like a tracking device. Fed. R. Crim. P. 41(b)(4). In support, the Government contends that like a tracking device, the NIT was placed onto the FBI's computer server located in the district from which the magistrate judge issued the search warrant, the Eastern District of Virginia. Defendant's computer "electronically traveled" to the Eastern District of Virginia where it logged onto the Target Website and accessed the FBI's server that was hosting the Target Website, and then took the NIT through the TOR network and back to Defendant's physical computer, for the purpose of locating it.

This Court does not agree with the Government's argument that the warrant was permitted under Rule 41(b) because the NIT operated like a tracking device. Rule 41(b)(4) gives the magistrate judge authority "to issue a warrant to install within the

---

[2] After the warrants in this case were issued, Rule 41(b) was amended, effective December 1, 2016, to add Subsection (6), which provides:

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

The Amendment would have provided the magistrate judge with jurisdiction to issue the NIT warrant at issue here.

district a tracking device . . . to track the movement of a person or property located within the district, outside the district, or both." Fed. R. Crim. P. 41(b)(4). Rule 41(b)(4) defines tracking device as the meaning set forth in 18 U.S.C. § 3117(b). Under 18 U.S.C. § 3117(b), a tracking device is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117. Under the comments to Rule 41(b)(4), the magistrate judge's authority to approve a warrant for installation and use of a tracking device includes the authority to permit entry into an area where there is a reasonable expectation of privacy, install the tracking device, and maintain and remove the device. The comments make clear that the "Committee did not intend by this amendment to expand or contract the definition of what might constitute a tracking device" and that the "amendment is based on the understanding that the device will assist officers only in tracking the movements of a person or property within the district of issuance, or outside the district." Fed. R. Crim. P. 41(b)(4) (comments).

The NIT, however, does not merely track movements of property inside and outside the district. It causes a user's computer to download instructions from the Target Website. (Def.'s Ex. A ¶ 33). The instructions, which comprise the NIT are designed to cause the user's "activating" computer to transmit not the movement of a person or property, but rather the user's IP address, the type of operating system running on the computer, the activating computer's host name, the activating computer's operating system user name, and the activating computer's media access control address.

(Def.'s Ex. A ¶ 34). To the extent that the NIT could be said to be tracking movement of property in the form of information, the NIT is not merely tracking, NIT is causing the movement of the information from the user's computer back to a computer controlled by the government in the Eastern District of Virginia. (Def.'s Ex. A ¶ 36). Moreover, even assuming that the initial installation of the tracking device occurred on the government-control computer in the Eastern District of Virginia, Defendant's computer was never installed with NIT in the Eastern District of Virginia. The NIT was installed on Defendant's computer in Georgia and it never left Georgia. While each of the bits of information obtained by the NIT can help in conjunction with other investigative tools to lead officers to discover the location of a computer which may have been used to access pornography, categorizing obtaining the information "as tracking of the movement of a person or property" or even information is a stretch that this Court is unwilling to make. The Court therefore concludes that the NIT is not merely tracking, but searching the user's computer for data it wants and then sending it back to itself. (Def.'s Ex. A ¶ 36); Accord United States v. Gaver, No. 3:16-CR-88, 2017 WL 1134814, at *9 (S.D. Ohio. Mar. 27, 2017) (concluding that because the NIT did more than provide location information, the NIT is more than a tracking device); United States v. Pawlak, No. 3:16-CR-306-D(1), 2017 WL 661371, at *5 (N.D. Tex. Feb. 17, 2017); United States v. Kahler, No. 16-CR-20551, 2017 WL 586707, at *6 (E.D. Mich. Feb. 14, 2017) (concluding that the NIT was more than a tracking device and instead, was a surveillance device); United States v. Allain, No. 15-CR-10251, 2016

WL 5660452, at *10-11 (D. Mass. Sept. 29, 2016); United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *5-6 (W.D. Wash. Jan. 28, 2016)(concluding that Rule 41(b)(4) did not apply because defendant never controlled the government-controlled computer, defendant's computer was never physically located within the Eastern District of Virginia); United States v. Adams, No. 6:16-CR-11-Orl-40GJK, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10, 2016) (finding that the NIT is not a tracking device because it does not track, but rather searches for information); Fed. R. Crim. P. 41(b)(4), comments to the Rule (explaining that the Rule 41(b)(4) "is based on the understanding that the device will assist officers *only* in tracking the movements of a person or property within the district of issuance, or outside the district"); but see, e.g., United States v. Austin, No. 3:16-CR-00068, — F. Supp. 3d —, 2017 WL 496374, at *4-5 (M.D. Tenn. Feb. 2, 2017) (concluding that warrant was authorized under Rule 41(b)(4) because NIT was a tracking device); United States v. Jean, 207 F. Supp. 3d 920, 938-43 (W.D. Ark. 2016) (same).

Defendant argues suppression is warranted due to the violation of Rule 41 because the violation rises to a constitutional magnitude and the warrant is void *ab initio*. In support, Defendant contends that suppression is required because jurisdictional violations of Rule 41 rise to the level of constitutional magnitude since they deal with substantive judicial authority and not merely procedure. Defendant does not cite any authority from the Eleventh Circuit supporting his position and instead relies upon cases from the Tenth Circuit and the District of Massachusetts to support his

view. See United States v. Krueger, 809 F.3d 1109, 1126 (10th Cir. 2015); United States v. Levin, 186 F. Supp. 3d 26 (D. Mass. 2016).

Authority from the Eleventh Circuit does not support the view that constitutional violations of Rule 41 automatically require suppression of evidence. The Eleventh Circuit has concluded:

> Unless a *clear* constitutional violation occurs, noncompliance with Rule 41 requires suppression of evidence only where (1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule.

United States v. Gerber, 994 F.2d 1556, 1560 (11th Cir. 1993) (quoting United States v. Stefanson, 648 F.2d 1231, 1235 (9th Cir. 1981) (emphasis added)). Thus, suppression may be required in the case of clear constitutional violations, but no clear constitutional violation occurred here.[3] See, e.g., United States v. Brown, 569 F. App'x 759, 763

[3] Likewise, the Tenth Circuit's holding in United States v. Krueger cited by Defendant does not persuade the Court that evidence should be excluded in every case where there is a void search warrant. Rather than determining that the warrant was void merely because the magistrate judge lacked jurisdiction to authorize the warrant, the Tenth Circuit engaged in more extensive analysis. In that case, the government agents obtained a warrant which blatantly violated Rule 41(b). There, after government agents obtained a warrant from a United States magistrate judge in Kansas to search the defendant's residence in Kansas for items that may be used to depict child pornography such as computers and cellular phones, the agents learned that the defendant was visiting a friend in Oklahoma City and that the defendant's cellular phone and computer were not in the residence. Krueger, 809 F.3d at 1111. As a result, the agents obtained a second warrant from a second United States magistrate judge in Kansas authorizing law enforcement to search the Oklahoma residence where the defendant was staying and the defendant's automobile, which was parked outside the residence. Krueger, 809 F.3d at 1111. Instead of just deeming that the extra-territorial warrant was void and that the evidence obtained as a result of the search should be suppressed, however, the Tenth Circuit engaged in a more extensive

(11th Cir. 2014) (explaining that Rule 41(b) violation did not result in suppression of evidence even if Rule 41 is viewed as an extension of the Fourth Amendment, because obtaining a warrant in state court was not a clear constitutional violation given that Rule 41(b) did not clearly address issue of warrants obtained by state officers). Indeed, as shown by the litany of case law analyzing the validity of the Eastern District of Virginia warrant that followed, the Government could not have engaged in a clear constitutional violation because the violation of Rule 41(b) was far less than clear. Indeed, numerous cases have determined that the NIT warrant did not violate Rule 41(b) at all because the NIT is a tracking device as contemplated by Rule 41(b)(4). See, e.g., United States v. Austin, No. 3:16-CR-00068, 2017 WL 496374, at *4-5, 7-8 (M.D. Tenn. Feb. 2, 2017); United States v. Jones, No. 3:16-CR-026, 2017 WL 511883, at *3 (S.D. Ohio February 2, 2017); United States v. Bee, No. 16-00002-01-CR-W-GAF, 2017 WL 424905, at *3-4 (W.D. Mo. Jan. 13, 2017); United States v. Sullivan, No. 1:16-CR-270, 2017 WL 201332, at *5 (N.D. Ohio Jan. 18, 2017); United States v. McLamb, No. 2:16CR92, 2016 WL 6963046, at *6 (E.D. Va. Nov. 28, 2016); United States v. Jean, 207 F. Supp. 3d 920, 937-38 (W.D. Ark. 2016); U.S. v. Matish, 193 F. Supp. 3d 585, 612-13 (E.D. Va. 2016).

---

analysis. Similar to the approach in the Eleventh Circuit, the Tenth Circuit explained that if the Court determines that the Rule 41 violation is not of constitutional import, then the Court would determine whether the defendant can establish that, as a result of the Rule 41 violation that "(1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional or deliberate disregard of a provision in the Rule." Krueger, 809 F.3d at 1113.

Furthermore, even assuming Defendant could establish prejudice by showing that the search might not have occurred if the Virginia magistrate judge had not issued the warrant, Supreme Court precedents persuade this Court that application of the exclusionary rule is not appropriate in this case. The Supreme Court analyzed an analogous issue in Herring v. United States, 555 U.S. 135 (2009). In that case, the police officers arrested the defendant based upon their belief that there was a valid arrest warrant in existence and then discovered a gun and drugs within Herring's possession during a search incident to arrest. Herring, 555 U.S. at 137-38. Unbeknownst to the arresting officers, the arrest warrant had been rescinded, but the computer had not been updated to reflect the recall of the warrant. Id. The defendant was subsequently indicted for illegally possessing the gun and drugs. Herring, 555 U.S. at 138. When analyzing the case, the Supreme Court made clear that "the exclusionary rule is not an individual right and applies only where it results in appreciable deterrence" of misconduct by law enforcement. Herring v. United States, 555 U.S. 135, 140-41 (2009). The Supreme Court opined that where the "application of the exclusionary rule could provide some incremental deterrent, the possible benefit must be weighed against its substantial costs." Herring, 555 U.S. at 141; United States v. Bishop, No. 15-15406, — F. App'x —, 2017 WL 1208403, at *6 (11th Cir. Apr. 3, 2017) (holding that just because a Fourth Amendment violation has occurred does not automatically mean that evidence is excluded and that instead, the "application of the exclusionary rule depends on a cost-benefit analysis that takes into account the deterrent value served by

suppression and the substantial social costs generated by the rule") (citing Davis v. United States, 564 U.S. 229, 237 (2011)). The benefit of deterrence must outweigh the costs. Herring, 555 U.S. at 141. The Court then reasoned that the potential cost of applying the rule is "letting guilty and possibly dangerous defendants go free" and that the costly toll "upon truth-seeking and law enforcement objectives presents a high obstacle for those urging its application." Herring, 555 U.S. at 141. On the other hand, the Court reasoned that the prevention of the merely negligent conduct at issue would not sufficiently advance the cause of deterrence to outweigh the cost of applying the exclusionary rule. Herring, 555 U.S. at 147-48. The Court further reasoned that the negligent conduct was not so culpable as to require exclusion. Herring, 555 U.S. at 147-48.

Likewise, in Arizona v. Evans, 514 U.S. 1 (1995), the Supreme Court evaluated whether evidence seized incident to arrest should be excluded where the defendant's arrest warrant had been quashed by the Court and the Court may have failed to communicate that the warrant had been quashed to law enforcement. Id. at 4-5. There, the Court determined that the deterrent function of the exclusionary rule would not be served by suppressing the evidence. Id. at 14. First, the Court noted that the exclusionary rule was historically designed as a means of deterring police misconduct, not mistakes by court employees. Id. The Court next explained that there was no evidence in that case that court employees were inclined to ignore or subvert the Fourth Amendment or that lawlessness among court employees supported the application of the

extreme sanction of exclusion. Given that employees were not adjuncts to the law enforcement team, there was no basis for believing that application of the exclusionary rule would have a significant impact on court employees responsible for informing the police that a warrant had been quashed. Id. at 15.

Applying the Supreme Court's reasoning to the facts of this case, even if it is determined that the underlying warrant is void, the purposes of the exclusionary rule are not served by suppressing evidence. Given the lack of Government misconduct, there is little deterrent value to be served by applying the exclusionary rule in this case. As noted above, there is no evidence that the Government's pursuit of the search warrant amounted to an intentional and deliberate disregard of the Rule. Jurists are still disagreeing about whether the warrant violated Rule 41(b) and whether the warrant could be considered to be for purpose of installing a tracking device. Here, the Government sought a warrant by a neutral and detached magistrate judge who is independently responsible for following the law. There is no argument here that the Government misled the magistrate judge, omitted necessary facts, or otherwise obtained the warrant in bad faith. United States v. Shumaker, 479 F. App'x 878, 882-83 (11th Cir. 2012) (declining to suppress evidence obtained in violation of Rule 41 because there was no evidence that the government obtained the evidence in bad faith); Gaver, 2017 WL 1134814, at *10-12 (refusing to find bad faith where courts have disagreed on the issue of whether or not the NIT warrant at issue in this case complied with Rule 41(b) and noting that the agent did exactly what he was required to do, "gathered

evidence, and then submitted a very detailed warrant affidavit, explaining how the NIT would work . . . ."); Austin, 2017 WL 496374, at *4-5, 7-8 (explaining that given the lack of clear authority on whether warrant was authorized under Rule 41, the court could not conclude that the lack of authority would have been apparent to the agents and that any error about the magistrate judge's jurisdiction would rest with the magistrate judge and not with the agent). The agents did exactly what they are supposed to do–they supplied a detailed rendition of the facts and circumstances and allowed the magistrate judge to decide the legal issue of whether she could issue the warrant or not. The magistrate judge determined that she could do so. Thus, any mistake about jurisdiction rested with the magistrate judge, and there is simply no Government misconduct justifying imposition of the exclusionary rule. Just as in Arizona v. Evans, there is absolutely no indication here that application of the exclusionary rule would further the deterrent purpose of the rule because there is no hint that the agents did anything wrong or that magistrate judges would be deterred from erroneously assuming jurisdiction to approve a warrant where there was none. Thus, there is little deterrence value to weigh against the harmful effect of impeding law enforcement's efforts to prevent dissemination of child pornography images. Accordingly, this Court concludes that application of the exclusionary rule is unwarranted here and declines to follow the district court cases Defendant relies upon to support the notion that because the warrant was void ab initio, suppression of the evidence should be required. See United States v. Master, 614 F.3d 236, 241-43 (6th Cir. 2010) (rejecting former 6th Circuit precedent

that extraterritorial warrant was void ab initio and that evidence obtained pursuant to the warrant should be suppressed and instead reasoning that the balancing analysis in Herring should be applied); United States v. Taylor, No. 2:16-CR-00203-KOB-JEO-1, 2017 WL 1437511, at *14-17 (N.D. Ala. Apr. 24, 2017) (court balanced interests discussed in Herring and then applied good faith exception); United States v. Schuster, No. 1:16-CR-51, 2017 WL 1154088, at *8 (S.D. Ohio Mar. 28, 2017) (applying Herring balancing test to determine that evidence obtained as a result of the NIT warrant should not be suppressed); United States v. Perdue, No. 3:16-CR-305-D(1), 2017 WL 661378, at *4 (N.D. Tex. Feb. 17, 2017) (rejecting conclusion that good faith exception does not apply in the case of a void NIT warrant); United States v. Pawlak, No. 3:16-CR-306-D(1), 2017 WL 661371, at *5-6 & n.8 (N.D. Tex. Feb. 17, 2017) (discounting the defendant's argument that NIT warrant was void and instead applying the good faith exception); United States v. Kahler, No. 16-CR-20551, 2017 WL 586707, at *8 (E.D. Mich. Feb. 14, 2017) (declining to suppress evidence seized as a result of NIT warrant and focusing on fact that there was no police misconduct); United States v. Duncan, No. 3:15-CR-00414-JO, 2016 WL 7131475, at *3-4 (D. Ore. Dec. 6, 2016) (declining to exclude evidence obtained as a result of NIT warrant because to do so would have no deterrent affect on police conduct); United States v. Adams, No. 6:16-CR-11-Orl-40GJK, 2016 WL 4212079, at *7 (M.D. Fla. Aug. 10, 2016) (declining to follow cases holding that a violation of Rule 41(b) renders the warrant void ab initio and considering whether the warrant was obtained and executed in good faith).

For the aforementioned reasons, this Court also concludes that the good faith exception to the exclusionary rule also applies. In United States v. Leon, 468 U.S. 897 (1984), the Supreme Court crafted an exception to the exclusionary rule. Id. Under this exception, evidence discovered by an officer acting in objective good faith on a search warrant issued by a detached and neutral magistrate should not be suppressed even if the warrant is later found to have violated the Fourth Amendment. Leon, 468 U.S. at 926. The "good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization. United States v. Taxacher, 902 F.2d 867, 871 (11th Cir. 1990), citing Leon, 468 U.S. at 922. In making this determination, all of the circumstances . . . may be considered." Taxacher, 902 F.2d at 871. The good faith exception will not apply (1) "if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth," (2) "where the issuing magistrate wholly abandoned his judicial role," (3) where the "warrant [is] based on an affidavit 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable,'" and (4) where "a warrant [is] so facially deficient . . . that the executing officers cannot reasonably presume it to be valid." Leon, 468 U.S. at 923; Taxacher, 902 F.2d at 871. The "good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization. In making this

determination, all of the circumstances . . . may be considered." Leon, 468 U.S. at 922 n.23; Taxacher, 902 F.2d 871 ("Observing that the purpose of the exclusionary rule is to deter unlawful police conduct, the Court found that this purpose would not be served, and the rule should not be applied, when officers engage in 'objectively reasonable law enforcement activity."); United States v. Wright, 811 F. Supp. 1576, 1583-84 (S.D. Ga. 1993).

In this case, application of the good faith exception is warranted because agents acting on the search warrant could not have known that the Virginia magistrate judge authorizing the warrant did not have jurisdiction under Rule 41(b). Indeed, competent jurists have since disagreed as to whether the magistrate judge's issuance of the warrant exceeded her territorial jurisdiction as delineated in Rule 41(b). Compare, e.g., Gaver, 2017 WL 1134814, at *9 (concluding that warrant exceeded magistrate judge's authority under Rule 41(b)); Pawlak, 2017 WL 661371, at *5 (same); Adams, 2016 WL 4212079, at *6 (same); with Austin, — F. Supp. 3d —, 2017 WL 496374, at *4-5 (concluding that warrant was authorized under Rule 41(b)(4) because NIT was a tracking device); United States v. Jean, 207 F. Supp. 3d 920, 938-43 (W.D. Ark. 2016) (same). To date, the question remains unsettled. Therefore, application of the good faith exception is warranted. See United States v. Lara, 588 F. App'x 935, 939 (11th Cir. 2014) (applying good faith exception even though superior court may have lacked authority under state law to issue wiretap where warrant may have been outside superior court's territorial jurisdiction because given murky state of the law, officers reasonably relied on warrant

in good faith); United States v. Hickman, 83 F.3d 416 (4th Cir. 1996) (applying good faith exception where officers relied on facially valid arrest warrant even though the judge issuing the warrant did not have proper jurisdiction); Taylor, 2017 WL 1437511, at *16 (applying good faith exception because magistrate judge's mistaken belief that she had jurisdiction, absent any indicia of reckless conduct by the agents, did not warrant suppression and exclusion would serve little deterrent purpose where the mistaken conduct of the magistrate judge, not the officers, invalidated the warrant); Adams, 2016 WL 4212079, at *7 (applying good faith exception where evidence was obtained pursuant to NIT warrant because the parties devoted sixty pages of written argument to the issue and cited competing caselaw, and defendant failed to offer evidence that the agents possessed some unique knowledge rendering their reliance on the NIT warrant objectively unreasonable); see also Pawlak, 2017 WL 661371, at *6 (finding that the good faith exception applied after pointing out that it was far from clear at the time that the NIT warrant was obtained that the warrant violated Rule 41(b) and that several courts have occurred that the NIT warrant did not violate Rule 41(b)); United States v. Sullivan, No. 1:16-CR-270, — F. Supp. 3d —, 2017 WL 201332, at *8 (N.D. Ohio Jan. 18, 2017) (applying the good faith exception after noting that "given the varying treatment of the NIT warrant by district court and magistrate judges alike, the FBI agents can hardly be faulted for failing to understand the intricacies of the jurisdiction of federal magistrate judges."). Consequently, Defendant's Motion to Suppress should be **DENIED**. (Doc. 34).

MOTION TO DISMISS INDICTMENT

Defendant argues the Indictment against him should be dismissed because the Government engaged in unprecedented misconduct when it continued operating the TOR network and Target Website after seizing control of it. In support, Defendant contends that the Government's continued operation resulted in the further circulation of illicit pictures to the detriment of the child pornography victims. Defendant maintains that the Government need not continue to disseminate the child pornography in order to locate and apprehend the perpetrators and instead could have simply blocked access to the pictures when guilty parties clicked on the links to illicit images. The Government argues the conduct in this case does not warrant dismissal of the indictment because it was not so outrageous that it is fundamentally unfair and shocking to the universal sense of justice. In support, the Government points out that it did not create the child pornography site, it did not induce anyone to create an account or become members, it did not encourage individuals to download or possess child pornography, and it did not post any new images to the site.

Defendant invokes the outrageous government conduct defense. The defense "focuses on whether the tactics employed by law enforcement officials to obtain a conviction for conduct beyond the defendant's predisposition violate the Fifth Amendment's due process guarantee." United States v. Dixon, 626 F. App'x 959, 962-63 (11th Cir. 2015). "To constitute a constitutional violation, the law enforcement

technique must be so outrageous that it is fundamentally unfair and shocking to the universal sense of justice mandated by the Due Process Clause of the Fifth Amendment." United States v. Ofshe, 817 F.2d 1508, 1516 (11th Cir. 1987); see also United States v. Arango, 853 F.2d 818, 828 (11th Cir. 1988) (finding that "[o]utrageous government conduct occurs when law enforcement obtains a conviction for conduct beyond the defendant's predisposition by employing methods that fail to comport with due process guarantees." United States v. Jayyousi, 657 F.3d 1085, 1111-12 (11th Cir. 2011). When analyzing whether the conduct is sufficiently outrageous, "the totality of the circumstances must be considered with no single factor controlling." Ofshe, 817 F.2d at 1516. The defense may be invoked only in the rarest circumstances. Ofshe, 817 F.2d at 1516. Indeed, the Eleventh Circuit has never found that the government's conduct rose to the level of outrageousness required for the defense to succeed. Dixon, 626 F. App'x at 963 (citing Jayyousi, 657 F.3d at 1111). "The Supreme Court has also made it abundantly clear that the limitations of the Due Process Clause . . . come into play only when the Government activity in question violates some protected right of the defendant." United States v. Farias, 836 F.3d 1315, 1325 (11th Cir. 2016) (citing Hampton v. United States, 425 U.S. 484, 490 (1976) (explaining that if the police engage in illegal activity in concert with a defendant beyond the scope of their duties the remedy lies, not in freeing the equally culpable defendant, but in prosecuting the police under the applicable provisions of state or federal law)). Thus, a defendant's

allegations that the Government's conduct harmed individuals other than the defendant fail to establish a violation of the defendant's due process rights. Farias, 836 F.3d at 1325-26 (rejecting defendant's argument that the government's action violated his due process rights where defendant argued that government sting operation benefitted tobacco companies and harmed public health by making cigarettes available at a below-market price).

Based on all the facts and circumstances as alleged in this case, Defendant fails to demonstrate that the Government's conduct was outrageous. While this Court agrees with Defendant that perpetuating the distribution of the alleged child pornography on the site is a troubling aspect of the Government's investigative efforts, this Court cannot conclude that the Government's conduct violated Defendant's due process rights. The main reason the Court finds Defendant's argument is unpersuasive, however, is that there is nothing about the Government's actions that was unfair to this Defendant. First, there is no allegation that the Government's investigating agents lured Defendant into the site or the world of child pornography or that Defendant did not have any prior predilection for child pornography. There is no allegation that the Government solicited Defendant to purchase child pornography or encouraged Defendant to visit the Target Website being operated by the Government. Based on the undisputed facts alleged in the warrant, it would be highly unlikely for an innocent user to stumble onto the website without knowing its purpose and content. A user may not simply perform a Google

search to locate the Target Website. (Def.'s Ex. A ¶ 10). The Target Website is a hidden service and does not reside on the traditional or open internet and may only be accessed via the TOR network. (Def.'s Ex. A ¶ 10). Even after connecting to the TOR network, the user must know the web address of the website in order to access the Target Website. (Def.'s Ex. A ¶ 10). A user may obtain the web address for the Target Website by communicating with other users on the Target Website's bulletin board, from internet postings describing the sort of content available on the website as well as the website's location, or a hidden services page dedicated to pedophilia and child pornography. (Def.'s Ex. A ¶ 10). Additionally, accessing the website requires numerous affirmative steps by the user and the user must choose to continue after receiving disclaimer about the Target Website's content and requirements for maintaining privacy. (Def.'s Ex. A ¶¶ 10, 13). Indeed, in order to access the site, the user must do another affirmative act in order to protect his or her privacy; the user must install TOR software either by downloading an add-on to the user's web browser or by downloading the free browser bundle. (Def.'s Ex. A ¶¶ 7-8).

Defendant contends that the continued operation of the Target Website was sufficiently outrageous because there were other options that the Government could have employed which would not have harmed innocent third parties, such as child pornography victims, as much. Defendant suggests that the Government could have instead denied users accessing the Target Website the illegal content of the site. This

Court disagrees that the Government's failure to choose an alternative method warrants dismissal of the Indictment. Courts give deference to the Government's choice of investigatory methods. United States v. Kim, No. 16-CR-191 (PKC), 2017 WL 394498, at *2, 4 (E.D.N.Y. Jan. 27, 2017) (citing United States v. Al Kassar, 660 F.3d 108, 121 (2d Cir. 2011)); United States v. Owens, No. 16-CR-38-JPS, 2016 WL 7079617, at *5 (E.D. Wis. Dec. 5, 2016) (explaining that the court was taking no position on the propriety of the government's actions in operating the Playpen website during the course of the investigation because the court did not fully understand the complexity of child pornography investigations in today's technology-filled world and would not lightly second guess the investigatory techniques of trained experts). In that vein, the Eleventh Circuit has a history of being deferential to investigatory methods and has opined that "[g]overnment infiltration of criminal activity is a recognized and permissible means of investigation and frequently requires that the government agent furnish something of value to the criminal." United States v. Sanchez, 138 F.3d 1410, 1413 (11th Cir. 1998). The Eleventh Circuit has found, for instance, that the government's conduct was not outrageous or intolerable when the government, in an effort to catch illegal drug distributors, allowed some marijuana out on the streets. See United States v. Rogers, 701 F.2d 871, 872 n.1 (11th Cir. 1983). Additionally, the Eleventh Circuit has held that a defendant who was convicted for drug offenses while in jail did not show sufficiently outrageous conduct even though the government allowed a fellow inmate to run an

illegal prison gambling operation while assisting the government with investigation of drug trafficking inside the prison. United States v. Becker, 196 F. App'x 762, 763 (11th Cir. 2006). The government allowed the continuation of the gambling operation for the purposes of allowing the fellow inmate to maintain interaction with other prisoners and so that the inmate could have the financial means to complete a drug transaction with the defendant. Id. at 763.

Likewise, in United States v. Tobias, 662 F.2d 381 (5th Cir. 1981),[4] the DEA, in order to pursue undercover investigations of clandestine laboratory drug operators, established a chemical supply company in a mid-western state. Id. at 383. The DEA received orders via telephone and mail for various chemicals which could be used in the manufacture of controlled substances. Id. The supply company placed in advertisement in High Times Magazine offering "over-the-counter sales of chemicals and laboratory equipment." Id. The defendant, Tobias, telephoned the supply company and placed an order for chemicals. Id. When Tobias complained that he wanted to cancel his order because he could not make cocaine without more knowledge and a lot more equipment, a special agent empathized with him that making cocaine was difficult and expensive and recommended that almost anything would be cheaper and easier to manufacture than cocaine, including amphetamines. Id. The agent suggested that Tobias make

[4] In Bonner v. City of Prichard, 661 F.2d 1206, 1209 (11th Cir. 1981) (en banc), this court adopted as binding precedent all decisions of the former Fifth Circuit handed down prior to October 1, 1981.

Phencyclidene (PCP) instead. Id. Tobias cancelled his order and asked that the agent send him everything needed to make PCP. Id. at 384. After receiving the chemicals and the formula for PCP, Tobias contacted the supply company thirteen times to discuss problems encountered during the manufacturing process. Id.

The Eleventh Circuit concluded that it was not outrageous for the government to place an ad in High Times, to ship the necessary chemicals to Tobias' home, or to give him step by step advice on how to make PCP on more than thirteen occasions. Id. at 387. In reaching that conclusion, the Circuit focused on the fact that the DEA did not pursue Tobias; Tobias not only initiated the contact with the government, but also was an active participant in the scheme when he made the thirteen contacts to the DEA. Id.

While this Court acknowledges that there may be some differences in scale between the government operations in the aforementioned cited Eleventh Circuit cases and the instant case, similar child pornography investigation operations by government agents have not proved sufficiently outrageous to amount to a due process violation. For instance, in United States v. Mitchell, 915 F.2d 521, 522-24 (9th Cir.1990), the Ninth Circuit evaluated government agents' conduct in targeting individuals suspected of purchasing pornography from commercial distributors, gathering the names of individuals who responded to advertisements placed by the government in sexually oriented magazines, and collecting the names of friends, associates, and correspondents of individuals who had been arrested for violating pornography laws. Id. at 524. The

government sent targeted individuals applications or questionnaires in connection with solicitation for possible membership with various undercover organizations established by the government, such as "Love Land," "Crusaders for Sexual Freedom," and the "American Hedonist Society." Id. at 524. The questionnaires were also designed to ascertain potential interest in child pornography and individuals believed to have interest in child pornography/pedophilia were solicited again with a catalog and order form prepared by the government. Id. at 525-26. In that case, the defendant purchased a child pornography magazine he found in the catalog and received the magazine. Id. at 525-26. The Ninth Circuit concluded that the government's actions did not violate the defendant's due process rights or notions of fundamental fairness because the defendant was not coerced or threatened into buying child pornography, the defendant voluntarily responded to the solicitation without government prodding, and the defendant had previously ordered an illicit child pornography magazine. Id. Other circuits have reached similar conclusions. See United States v. Musslyn, 865 F.2d 945, 946-47 (8th Cir. 1989); United States v. Driscoll, 852 F.2d 84, 85-86 (3d Cir. 1988) (the government's solicitation of child pornography to defendant was not outrageous enough to amount to a due process violation where the defendant was clearly predisposed to collect child pornography and government did nothing to because the nature of the production, distribution, and sale of child pornography itself justifies such uncover operations).

Likewise, in the instant case, there is no allegation here that the Government directly solicited Defendant or otherwise prodded him to access the site. Given the undisputed difficulty in locating the Target Website and the affirmative steps the user must take to retrieve its information, it may be inferred that individuals who accessed the Target Website were highly motivated to do so. There is no indication that the Government's continued operation of the Target Website actually caused Defendant to allegedly commit a crime that he would not otherwise have committed, or that Defendant would have been deterred from allegedly viewing child pornography if the images on the Target Website had been unavailable.

Furthermore, the impact of the Government's continued operation of the Target Website on third parties, such as child pornography victims, does not tip the balance of the equation in this case because the harm to the child pornography victims does not result in any unfairness to Defendant or otherwise harm Defendant's due process rights. Farias, 836 F.3d at 1325-26 (11th Cir. 2016) (citing Hampton, 425 U.S. at 490). Notwithstanding the fact that the Government did not do anything to entice Defendant, the Court cannot conclude that the Government's conduct here was sufficiently outrageous to warrant dismissal of the Indictment. The Government did not design a website or put illegal content on the website for the purposes of enticing users; the Target Website was already in existence and operational at the time the Government took it over. (Def.'s Ex. A ¶¶ 11-30). Additionally, the Target Website already had

allegedly illegal content; there is no allegation here that the Government added additional illicit content as a part of its scheme. (Id.). The Government simply operated the Target Website for a short time period (no more than two weeks) in an effort to learn the identities of additional users. (Def.'s Ex. A ¶ 30; Def.'s Ex. C ¶ 24). Furthermore, this Court cannot fault the Government for its chosen method of investigation because it is not difficult to infer the inferiority of other investigatory methods suggested by Defendant. For instance, Defendant suggests that the Government should not have allowed access to the illegal images and should have instead allowed an error message to appear. The repeated error messages denying the users the content they expect to receive might have caused the users to suspect that the website was commandeered by law enforcement and such users might share their suspicions with other users. Indeed, the website itself allows users to send other users private messages. (Def.'s Ex. A ¶ 20). This in turn might have decreased the number of users caught by law enforcement or suspecting users might conceal the evidence of their crimes. Therefore, based on the facts as alleged by Defendant, the Government's actions with respect to him were not so outrageous as to amount to a violation of due process. This Court's conclusion is consistent with every district court which has had opportunity to consider whether the Government's continued operation of the Target Website violated the defendant's due process. United States v. Pawlak, No. 3:16-CR-306-D(1), 2017 WL 661371, at *7-8 (N.D. Tex. Feb. 17, 2017) (concluding that government's operation of the target website

did not violate due process because the government did not create the website, did not alter the website's functionality, did not add child pornography, did not actively solicit new users, but rather simply maintained existing structure); United States v. Kim, No. 16-CR-191 (PKC), 2017 WL 394498, at *3-4 (E.D.N.Y. Jan. 27, 2017) (explaining that the continued operation of the target website was not sufficiently outrageous to offend due process principles because defendant did not show that FBI's operation of target website would have resulted in the commission of child pornography crimes which would not have otherwise been committed or that the government's conduct caused defendant to commit crimes he would not have committed); United States v. Vortman, No. 16-CR-00210-THE-1, 2016 WL 7324987, *4-6 (N.D. Cal. Dec. 16, 2016); United States v. Owens, No. 16-CR-38-JPS, 2016 WL 7079617, at *4-5 (E.D. Wis. Dec. 5, 2016) (rejecting defendant's due process argument because the government did not create the Playpen website, the government did not coerce the defendant into receiving and possessing child pornography, and the government's conduct in maintaining the Playpen website is far attenuated from the evidence used to prosecute the defendant); United States v. Allain, No. 15-CR-10251, — F. Supp. 3d —, 2016 WL 5660452, at *13 (D. Mass. Sept. 29, 2016) (concluding that while investigation of child pornography had disturbing consequences because the pornography distributed by the government might live on and be redistributed in the internet for indefinite amount of time, investigation was not outrageous because the difficulty of identifying individuals accessing child

pornography online forces investigators to make difficult choices about how to investigate and prosecute the crime). Therefore, this Court concludes that Defendant's Motion to Dismiss should be **DENIED**. (Doc. 33).

This Court also concludes that Defendant is not entitled to a hearing on the Motion to Dismiss because, even assuming the facts as alleged by Defendant, the Government's acts were not so outrageous as to amount to a due process violation. See, e.g., Owens, 2016 WL 7079617, at *5 (declining to hold hearing on motion to dismiss indictment due to government's outrageous conduct in operating the Playpen website because the defendant was not entitled to dismissal even irrespective of any purported factual disputes between the parties); see also United States v. Verch, 307 F. App'x 327, 330 (11th Cir. 2009) (citing United States v. Holloway, 778 F.2d 653, 658-59 (11th Cir. 1985) (affirming district court's refusal to dismiss indictment due to defendant's claims of prosecutorial misconduct even though district court did not hold a hearing on the matter where defendant had not raised a material fact which, if resolved in accordance with his contentions, would entitle him to relief)). Accordingly, Defendant's request for a hearing is **DENIED**. (Doc. 33).

CONCLUSION

Based on the foregoing reasons, this Court **RECOMMENDS** that Defendant's Motion to Dismiss the Indictment and Motion to Suppress should be **DENIED**. (Docs. 33, 34). Defendant's request for a hearing on the Motion to Dismiss the Indictment is

DENIED. (Doc. 33).

SO ORDERED AND REPORTED AND RECOMMENDED this 1st day of May, 2017.

/s/ Linda T. Walker
LINDA T. WALKER
UNITED STATES MAGISTRATE JUDGE